MINIMUM NECESSARY

[*45 CFR 164.502(b), 164.514(d)*]

Background

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

How the Rule Works

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the

future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

Uses and Disclosures of, and Requests for, Protected Health Information. For uses of protected health information, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification.

For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required.

For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly.

Of course, where protected health information is disclosed to, or requested by, health care providers for treatment purposes, the minimum necessary standard does not apply.

Reasonable Reliance. In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).

- Another covered entity.

- A professional who is a workforce member or business associate of the covered entity holding the information and who states that the information requested is the

minimum necessary for the stated purpose.

- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The Rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

MINIMUM NECESSARY

Frequently Asked Questions

Q: How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

A: The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

Q: Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

A: No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

Uses of protected health information for treatment are not exempt from the minimum necessary standard. However, the Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to identifiable health information within the covered entity. The Rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity may develop role-based access policies

that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Q: Do the HIPAA Privacy Rule's minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training?

A: No. The definition of "health care operations" in the Privacy Rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

Q: Must the HIPAA Privacy Rule's minimum necessary standard be applied to uses or disclosures that are authorized by an individual?

A: No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. For example, if a covered health care provider receives an individual's authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of 45 CFR 164.508.

Q: Are providers required to make a minimum necessary determination to disclose to Federal or State agencies, such as the Social Security Administration (SSA) or its affiliated State agencies, for individuals' applications for Federal or State benefits?

A: No. These disclosures must be authorized by an individual and, therefore, are exempt from the HIPAA Privacy Rule's minimum necessary requirements. Furthermore, use of the provider's own authorization form is not required. Providers can accept an agency's authorization form as long as it meets the requirements of 45 CFR 164.508 of the Privacy Rule. For example, disclosures to SSA (or its affiliated State agencies) for purposes of determining eligibility for disability benefits are currently made subject to an individual's completed SSA authorization form. After the compliance date, the current process may continue subject only to modest changes in the SSA authorization form to conform to the requirements in 45 CFR 164.508.

Q: Doesn't the HIPAA Privacy Rule's minimum necessary standard conflict with the HIPAA transactions standards?

A: No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the transactions standards, including disclosures of all data elements that are required or situationally required in those transactions. See 45 CFR 164.502(b)(2)(vi). However, covered entities have significant discretion as to the information included in the transactions as optional data elements. Therefore, the minimum necessary standard does apply to the optional data elements. The transactions standard adopted for the outpatient pharmacy sector is an example of a standard that uses optional data elements. The health plan, or payer, currently specifies which of the optional data elements are needed for payment of its particular pharmacy claims. The health plan or its business associates must apply the minimum necessary standard when requesting this information. In this example, a pharmacist may reasonably rely on the health plan's request for information as the minimum necessary for the intended disclosure. For example, as part of a routine protocol, the name of the individual may be requested by the payer as the minimum necessary to validate the identity of the claimant or for drug interaction or other patient safety reasons.

Q: Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time an entire medical record is disclosed?

A: No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the protected health information.

Q: A provider might have a patient's medical record that contains older portions of a

medical record that were created by another or previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

A: Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to protected health information to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. In this case, appropriate training of employees may be sufficient. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the Privacy Rule.

Q: Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of protected health information it makes to another covered entity?

A: Covered entities are required to apply the minimum necessary standard to their own requests for protected health information. One covered entity may reasonably rely on another covered entity's request as the minimum necessary, and then does not need to engage in a separate minimum necessary determination. See 45 CFR 164.514(d)(3)(iii).

However, if a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered entities to negotiate a resolution of the dispute as to the amount of information needed. Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with another covered entity making a request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

Q: May a covered entity accept documentation of an external Institutional Review Board's (IRB) waiver of authorization for purposes of reasonably relying on the request as the minimum necessary?

A: Yes. The HIPAA Privacy Rule explicitly permits a covered entity to reasonably rely on a researcher's documentation of an Institutional Review Board (IRB) or Privacy Board waiver of authorization pursuant to 45 CFR 164.512(i) that the information requested is the minimum necessary for the research purpose. See 45 CFR 164.514(d)(3)(iii). This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or from one that is associated with the covered entity.

Q: Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

A: A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.